LAPORAN TUGAS AUTOPSY PADA MATA KULIAH FORENSIK DIGITAL

Dosen Pengampu: Rizky Fenaldo Maulana, S.Kom., M.Kom.

Disusun Oleh :

Yayuk Agustina

1203210118

IF 01-01

PROGRAM STUDI INFORMATIKA

FAKULTAS INFORMASI

TELKOM UNIVERSITY SURABAYA

TAHUN AJARAN 2021/2022

HASIL YANG DIPEROLEH DAN KESIMPULAN DARI PERCOBAAN APLIKASI AUTOPSY

1. Di local disk D Membuat folder Cases selanjutnya di dalam folder cases membuat folder dengan nomor kasus 001 dan menambahkan semacam indikator jenis investigasi, dengan cara itu saya bisa melihat kasus saya yang mungkin tidak menegenali nomor kasusnya tetapi saya dapat mengenali tagnya jadi saya akan memberi tanda H,sedangkan jij ini tentang tag penyelidik dan XX ini adalah inisialnya aggota penyelidik.
2. Selanjutnya di folder 001-H-jij-XX ini akan membuat folder lagi yang terdiri Docs, Image, temp, Autopsy, Reports
3. Selanjutnya masuk kedokumen dan saya akan membuat dokumen teks baru yang berjudul 001-H-jij-XX-doc.txt, selanjutnya membuat dokumentasi kasus yang dibuka di notepad tekan f5 untuk memasukkan stempel waktu. dan sebelum keluar jangan lupa untuk disimpan.
4. Membuat file di dalam folder image, jadi membuat data yang dicurigai yaitu Exhibit001. selanjutnya klik dua kali pada Exhibit001 kemudian memindahkan data ke diroktori (ada di link youtube). dan selanjutnya menambahkan data SuspectData.dd-hashes.txt.
5. Selanjutnya open apk autopsy
6. Selanjutnya pilih yang new case
7. Isi case name : 001-H-jij-XX
8. Isi base directory : D:\CASES\001-H-jij-XX\Autopsy (alasan menggunakan nomor kasus adalah siapa pun yang membaca catatn ini melihat bawa catatan itu selalu berada di direktotri yang sama.
9. Pilih sigle user
10. Selanjutnya klik next
11. Selanjutnya isi number :001
    Name : nama
    Phone : isi nomor hp (agar sistem management tau akan menghubungi kesiapa kasus tersebut)
    Email : isi email
    organization analysis is being done for : CIA (menambahkan organisasi)
    Klik finish
12. Pilih specify new host name : Exhibit001 selanjutnya klik next
13. Klik disk image or VM file : adalah yang berada di folder image

sedangkan local disk unntuk membaca data secara langsung jadi

14. Selanjutnya pilih path image : D:\CASES\001-H-jij-XX\Image\SuspectData.dd
15. Pilih time zone wilayah
16. Isi hash value

    md5 : efbf30672c4eb3713b7f639f16944fd3

    SHA-256 : 6baed29520499d2d5c44c32a0f3a8a08cbe92c47b4e00101b1041d14f9a579e2

    Selanjutnya klik next
17. Pencarian hash lookup adalah kita dapat mengatur database hash dari file yang diketahui baik dan file buruk yang diketahui n serta dimana file yang diketahui baik kita dpat menggunakan data base hash untuk memfilter file yang kita tahu bagus sehingga tidak perlu lagi melihat di autopsy. hash juga dapat menambahkan database hash buruk yang diketahu dimana jika ada file yang cocok dengan hash buruk yang diketahui, maka file tersebut secara otomatis ditandai umtuk kita mininjau sehingga membuat penyeldikan menjadi sangat mudah

    klik file type identification ialah dapat mengatur jenis file yang ingin dicocokkan dalam pengaturan global
18. Selanjutnya klik next
19. Selanjutnya di exhibit001 kita dapat melihat gambar dan data mentah dari gambar yang dapat dilihat ditampilan hex (tampilan ascii)
20. klik launch in Hxd untuk menginstall / dowlod hxd
21. Penjelasan mengenai search misal kita ke suspectdata keyword lalu search CAT dia akan memunculkan beberapa pilihan cat. jika sudah kita pilih keyword hits lalu klik single literal keyword serch (disitu akan memunculkan kembali apa yang sudah kita search tadi) di suspectdata keyword search
22. Selanjutnya pada keyword search di cat klik kanan klik add file tag yaitu untuk menambahkan tag file lalu klik bookmark
23. Pilih tags, selanjutnya pilih bookmark, klik file tags disitu akan muncul yang telah kita bookmark tadi
24. Klik kanan pada file gambar yang telah di bookmark lalu pilih ekstract file maka file akan muncul pada penyimpanan image internal dan eksternal
25. Klik generate report untuk membuat laporan dan apa yang dilakukan pada beberapa jenis laporan yang berbeda selanjutnya klik html report kemudian akan memproses data yang dicurigai (suspectdata.dd) selanjutnya klik spesifik targged result untuk data yang dilaporkan yang dapat melakukan hasil yang diberi tags tertentu selanjutnya akan

melakukan hasil yang diberi tags khusus lalu klik centang bookmark dan klik finish untuk mengakhiri dan selanjutnya ada link akan menghasilkan laporan tentang data yang telah di tandai jika tautan di klik maka akan melihat file laporan dan itu memiliki meta data darimana kami memulai kasus forensik Aoutopsy semua lokasi yang harus sesuai dengan dokumentasi, dan kemudian di sisi kiri kami dapat melihat file yang diberi tags dan kami memiliki bookmart yang merupakan salah satu gambar kucing dengan metadatanya dan kemudian item penting juga ditaandai dengan metadatanya jika saya mengklik salah satu tautan itu, maka saya dapat melihat file secara langsung sehingga telah di ekspor dengan laporan kami.

Jadi kesimpulan yang saya dapat setelah melakukan uji coba Autopsy adalah setiap apa yang ingin dilakukan pada aplikasi autopsy contohnya seperti edit,bookmark,tags an lain sebaigainya, maka akan masuk ke file folder autopsy